JOURNAL OF NUMBER THEORY **65**, 197–205 (1997)
ARTICLE NO. NT972149

Digit Variance and Dedekind Sums

Kurt Girstmair

Institut für Mathematik, Universität Innsbruck, Technikerstrasse 25/7, A-6020 Innsbruck, Austria

Communicated by D. Zagier

Received February 14, 1996; revised January 13, 1997

Let $p \geqslant 3$ be a prime number, $b \geqslant 2$ a primitive root mod p and z an integer, $1 \leqslant z \leqslant p-1$. The digit expansion of z/p with respect to the basis b has a period consisting of the first $p-1$ digits $c_1, \ldots, c_{p-1}$. We express the variance σ^2 of

important tool in this investigation.

1. MAIN RESULTS

The classical Dedekind sums $s(b, n)$ go back to the 19th century and can be defined in an elementary way (cf. formula (4) below). Originally, however, they did not occur in an elementary context but in connection with deep results of complex analysis. Methods of complex analysis also supplied the first proof of the most important property of Dedekind sums, the so-called *reciprocity law* (cf. [5, Chap. 6]). In the 20th century a number of elementary proofs of this law were given. Moreover, it turned out that Dedekind sums have a meaning in an elementary mathematical context, too (cf. [2, p. 162ff; 5, p. 35ff]). In this article we exhibit another meaning, which is perhaps the most elementary considered so far.

Let b and n be natural numbers $\geqslant 2$, and z an integer with $1 \leqslant z \leqslant n-1$, $(z, n) = 1$. We consider the digit expansion of the rational number z/n with respect to the basis b, i.e.,

$$\frac{z}{n} = \sum_{j=1}^{\infty} c_j b^{-j},$$

where c_j is one of $0, 1, \ldots, b-1$, and c_j is different from $b-1$ for infinitely many indices j. In this way the sequence of digits c_j, $j = 1, 2, 3, \ldots$, is uniquely determined. Of course, it is a periodic sequence, and it has no preperiod if $(b, n) = 1$. In the sequel we always make this assumption. Let

0022-314X/97 $25.00

l be the order of $b \bmod n$, i.e., the smallest natural number k such that $b^k \equiv 1 \bmod n$. Then $(c_1, ..., c_l)$ is a period, and there is no shorter one. Let us consider this period as a sort of *random sequence* that takes values in $\{0, 1, ..., b-1\}$. Then the question arises what the *mean value*

$$m = \frac{1}{l} \sum_{j=1}^{l} c_j$$

and the *variance*

$$\sigma^2 = \frac{1}{l} \sum_{j=1}^{l} (c_j - m)^2$$

of this sequence may look like.

Let $\langle \bar{b} \rangle$ be the subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by the residue class $\bar{b}$ of $b \bmod n$. If $\overline{-1} \in \langle \bar{b} \rangle$, the mean value m is just the mean value of 0, 1, ..., $b-1$, i.e., $m = (b-1)/2$. For $n \geqslant 3$ this is due to the identity

$$c_j + c_{l/2+j} = b - 1, \qquad j = 1, ..., l/2,$$

which holds in this case (cf., e.g., [1]; cf. also the remark at the end of this section). The variance σ^2, however, does not possess such a simple shape. In order to describe it in the easiest cases, we introduce a modification of the above-mentioned Dedekind sums $s(b, n)$ (the advantages of this modification will become obvious soon): For relatively prime natural numbers b, n we put

$$S(b, n) = (n-1)(n-2)/6 - 2ns(b, n). \tag{1}$$

By means of the reciprocity law for Dedekind sums, we shall show:

THEOREM 1. *Let $n = p$ be a prime number $\geqslant 3$ and $b \geqslant 2$ a primitive root mod p. Then*

$$\sigma^2 = \frac{b^2 - 1}{12} - \frac{S(p, b)}{p - 1}.$$

Remark. The number b is a primitive root mod p if, and only if, the period length l takes its greatest possible value $l = p - 1$. This assumption implies $\overline{-1} \in \langle \bar{b} \rangle$, so $m = (b-1)/2$; moreover, σ^2 is independent of the numerator $z \in \{1, ..., p-1\}$ of z/p.

For the time being we fix $b \geqslant 2$. For a natural number n with $(n, b) = 1$ let $\sigma^2(n)$ be defined by

$$\sigma^2(n) = \frac{b^2-1}{12} - \frac{S(n,b)}{n-1}. \tag{2}$$

Hence, if $n = p \geqslant 3$ is a prime and b a primitive root mod p, $\sigma^2(p)$ is just the digit variance σ^2 of Theorem 1. Therefore, it seems natural to study the behaviour of $\sigma^2(n)$ for n tending to infinity. To this end put

$$\omega = \frac{b^2-1}{12}.$$

First one observes that the number $S(n, b)$ depends on the residue class of n mod b only—so it can take only a bounded number of values. Therefore,

$$\sigma^2(n) = \omega + O(1/n). \tag{3}$$

The next theorem describes the O-term more precisely. Put

$$\omega'(n) = \omega\left(1 - \frac{4(b-2)}{(b+1)(n-1)}\right),$$

which is $\leqslant \omega$ and, in general, close to $\omega(1-4/(n-1))$ (unless our fixed basis b is very small).

THEOREM 2. *Let* $(n, b) = 1$. *Then*

$$\omega \geqslant \sigma^2(n) \geqslant \omega'(n);$$

the upper bound is taken if, and only if, $n \equiv 1 \bmod b$, *whereas the lower bound is taken if, and only if,* $n \equiv -1 \bmod b$.

This theorem is a consequence of some elementary properties of the modified Dedekind sums $S(n, b)$. The proof of the following (stronger) result, however, uses the reciprocity law again.

THEOREM 3. *Let* $(n, b) = 1$.

1. *If* $n \not\equiv 1 \bmod b$, $\sigma^2(n) \leqslant \omega - \omega/(n-1)$; *here equality holds if, and only if,* b *is odd and* $n \equiv 2$ *or* $n \equiv (b+1)/2 \bmod b$.

2. *If* $n \not\equiv -1 \bmod b$, $\sigma^2(n) \geqslant \omega'(n) + \omega/(n-1)$; *here equality holds if, and only if,* b *is odd and* $n \equiv -2$ *or* $n \equiv (b-1)/2 \bmod b$.

Let us briefly look at the case when $\sigma^2(n)$ has an interpretation as a digit variance—so $n = p$ is a prime $\geqslant 3$ and b a primitive root mod p. We speak

of the *equidistributed case* if each of the numbers $0, ..., b-1$ occurs among the digits $c_1, ..., c_{p-1}$ with the same frequency. This situation can be characterized by the condition $p \equiv 1 \bmod b$ (we omit the proof). By Theorem 2, the variance σ^2 takes the value ω only in the equidistributed case. In all other cases σ^2 is smaller than ω. Indeed, Theorem 3 says that the difference $\omega - \sigma^2$ lies between $\omega/(p-1)$ and $3\omega/(p-1)$ (more precisely: $3\omega/(p-1) \cdot (b-2)/(b+1)$), with the exception of $p \equiv -1 \bmod b$, where this difference is (usually) close to $4\omega/(p-1)$.

Finally, we mention a case where the *mean value* m of the digits $c_1, ..., c_l$ of z/n differs from $(b-1)/2$: Let $n = p > 3$ be a prime $\equiv 3 \bmod 4$, and $l = (p-1)/2$. Then m takes one of the values $(b-1)/2 \cdot (1 \pm h/l)$, h denoting the class number of $\mathbb{Q}(\sqrt{-p})$ (cf. [1, Satz 11]).

2. PROOF OF THEOREM 1

We start with some preparations. For a natural number n and an integer k let $(k)_n$ denote the smallest nonnegative residue of $k \bmod n$; in other words, $(k)_n$ is completely determined by the conditions

$$(k)_n \equiv k \bmod n, \qquad (k)_n \in \{0, 1, ..., n-1\}.$$

Let b, n be relatively prime natural numbers. Then the Dedekind sum $s(b, n)$ is defined by

$$s(b, n) = \sum_{k=1}^{n-1} \frac{k}{n} \left(\frac{kb}{n} - \left[\frac{kb}{n} \right] - \frac{1}{2} \right) \tag{4}$$

(cf. [4, p. 146, formula (68.8)]); here $[x]$ means the largest integer $\leqslant x$, as usual. We use the symbol $(\cdots)_n$ to write $s(b, n)$ in a different way: Indeed, for any integer j,

$$\left[\frac{j}{n} \right] = \frac{j - (j)_n}{n}. \tag{5}$$

This identity and the well-known formulas

$$\sum_{k=1}^{n-1} k = \frac{(n-1)\, n}{2}, \qquad \sum_{k=1}^{n-1} k^2 = \frac{(n-1) n\, (2n-1)}{6},$$

yield

$$s(b, n) = \frac{1}{n^2} \sum_{k=1}^{n-1} k (kb)_n - \frac{n-1}{4}.$$

Hence

$$\frac{2}{n}\sum_{k=1}^{n-1}(k^2-k(kb)_n)=\frac{(n-1)(n-2)}{6}-2ns(b,n).$$

But the right side of this equation coincides with the right side of (1). Therefore,

$$S(b,n)=\frac{2}{n}\sum_{k=1}^{n-1}(k^2-k(kb)_n). \tag{6}$$

Next we recall the reciprocity law,

$$s(b,n)+s(n,b)=-1/4+(b/n+1/(bn)+n/b)/12 \tag{7}$$

(cf. [4, p. 148, formula (69.6)]). Because of (1), this formula is equivalent to the reciprocity law for the sums $S(b,n)$:

$$bS(b,n)+nS(n,b)=\frac{(b-1)(n-1)(b+n-1)}{6}. \tag{8}$$

Proof of Theorem 1. A central point in this proof is the observation that the digits of z/n can be expressed in terms of the symbol $(\cdots)_n$, too. Let $b\geqslant 2$, $(b,n)=1$, and z/n be as in Section 1 (in particular, $(z,n)=1$). For any integer $j\geqslant 0$ put

$$z_j=(zb^j)_n.$$

Then the digit c_j, $j\geqslant 1$, of z/n with respect to the basis b is given by

$$c_j=(z_{j-1}b-z_j)/n=(z_{j-1}b-(z_{j-1}b)_n)/n. \tag{9}$$

We leave the proof of (9) as an exercise, cf. [1, proof of Satz 1]. Let l be as in Section 1; i.e., $(c_1, ..., c_l)$ is the period of the fraction z/n. The integers $z_0, ..., z_{l-1}$ are all different and run through a subset of $\{1, ..., n-1\}$. This subset coincides with $\{1, ..., n-1\}$ if, and only if, n is a prime number and b is a primitive root mod n. In this case the sum

$$C(b,n)=\frac{1}{n^2}\sum_{k=1}^{n-1}(kb-(kb)_n)^2 \tag{10}$$

equals

$$\sum_{j=1}^{l}c_j^2,$$

LEMMA 5 (Dirichlet's approximation principle). *Let* $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_s) \in \mathbb{R}^s$, $q \in \mathbb{N}$, $t_0 \in \mathbb{R}^+$, *then there exist* $t \in \mathbb{R}$ *with* $\|t\boldsymbol{\alpha}\| < 1/q$ *and* $t_0 < t < t_0 q^s$, *where* $\|\cdot\|$ *denotes the distance from the nearest integer.*

4. PROOF OF THE THEOREM

We start with the Borel mean-value

$$B(t) = \frac{1}{\Gamma(k+1)} \int_0^\infty u^k e^{-u} E(\mathbf{a}; Xu^{\Sigma/2})\, du,$$

where $\Sigma = a_1 + \cdots + a_p$,

$$X = X(t) = K_1 (\log t)^{-a} (\log\log t)^{ca} \exp(A\sqrt{\log\log\log t}), \tag{4}$$

$$k = k(t) = K_2(\zeta + tX^{-1/\Sigma})^2 \tag{5}$$

with c as defined in (3), positive constants K_1, K_2, and real ζ to be specified later. We take formula (4.12) from Nowak [16],

$$B(t) \asymp X^\theta k^{(p-1)/4} \sum_{n=1}^{\infty} \rho(n)\, n^\theta e^{-c_1(nX)^{2/\Sigma}} \times \cos(\zeta(nX)^{1/\Sigma} + n^{1/\Sigma} t + \gamma_0) + O(k^{p/4 - 3/8}),$$

where γ_0 is some constant depending only on p.

We decompose this representation

$$B(t) \asymp X^\theta k^{(p-1)/4} \left\{ \sum_{n \in H} + \sum_{\substack{n \notin H \\ n \leqslant N}} + \sum_{n \geqslant N} \right\} \rho(n)\, n^\theta e^{-c_1(nX)^{2/\Sigma}} \times \cos(\zeta(nX)^{1/\Sigma} + n^{1/2} t + \gamma_0),$$

and apply Dirichlet's approximation theorem to the first sum. In Lemma 5 we choose $\alpha_n = n^{1/\Sigma}$. Let B_1 be a large positive integer, $H_1 = \# H(B_1)$ and $q \in \mathbb{N}$, $q \geqslant 2$ a parameter to be fixed later. Then there exists a number t in the interval

$$B_1 < t < B_1 q^{H_1}, \tag{6}$$

such that

$$\left\| \frac{1}{2\pi} n^{1/\Sigma} t \right\| < \frac{1}{q}$$

for all $\alpha_n \in H(B_1)$. From (6) we see that

$$H_1 \gg (\log t)(\log q)^{-1}. \tag{7}$$

Combining (7) and Lemma 3, a short calculation shows that

$$B_1 \gg (\log q)^{-a} (\log t)^a (\log\log t)^{-ca} \exp(-A\sqrt{\log\log\log t}).$$

We define

$$B_0 = c_0(\log q)^{-a} (\log t)^{a_1} (\log\log t)^{-ca} \exp(-A\sqrt{\log\log\log t})$$

with c_0 sufficiently small such that $B_0 < B_1$. We conclude that

$$|\cos(\zeta(nX)^{1/\Sigma} + n^{1/\Sigma}t + \gamma_0) - \cos(\zeta(nX)^{1/\Sigma} + \gamma_0)| < \frac{1}{q}$$

for all $n \in H(B_0)$. Therefore

$$\begin{aligned}
&\left| \sum_{n \in H_0} \rho(n)\, n^\theta e^{-c_1(nX)^{2/\Sigma}} \{\cos(\zeta(nX)^{1/\Sigma} + n^{1/\Sigma}t + \gamma_0) - \cos(\zeta(nX)^{1/\Sigma} + \gamma_0)\} \right| \\
&\quad \ll \sum_{n \leqslant B_0} \rho(n)\, n^\theta e^{-c_1(nX)^{2/\Sigma}} = \frac{1}{q} \int_{1^-}^{B_0} \exp(-c_1(uX)^{2/\Sigma})\, dS(u) \\
&\quad \ll \frac{1}{q} X^{-\theta} (\log B_0)^{p-1},
\end{aligned}$$

where

$$S(u) = \sum_{n \leqslant u} \rho(n)\, n^\theta \asymp u^\theta (\log u)^{p-1}. \tag{8}$$

Analogously,

$$\sum_{\substack{n \notin H \\ n \leqslant B_0}} \rho(n)\, n^\theta e^{-c_1(nX)^{2/\Sigma}} \ll \frac{1}{A^2} X^{-\theta} (\log B_0)^{p-1}.$$

Those n with $n \geqslant B_0$ contribute

$$\begin{aligned}
&\ll \sum_{n \geqslant B_0} \rho(n)\, n^\theta e^{-c_1(nX)^{2/\Sigma}} \\
&\ll B_0 (\log B_0)^{p-1} \exp(-c_1(B_0X)^{2/\Sigma}) \\
&\qquad + \int_{B_0}^{\infty} \exp(-c_1(uX)^{2/\Sigma})(uX)^{2/\Sigma - 1}\, XS(u)\, du.
\end{aligned}$$

Similarly, (2) and the consequent Proposition 1 give the first assertion of Theorem 3. The second assertion follows from the "complementary version" of this proposition, which the reader may write down himself.

PROPOSITION 1. *Let n, b be relatively prime natural numbers. If b is odd and $n \equiv 2 \bmod b$ or $n \equiv (b+1)/2 \bmod b$, then $S(n, b) = (b^2-1)/12$. If none of $n \equiv 1, 2, (b+1)/2 \bmod b$ holds, $S(n, b) > (b^2-1)/12$.*

Proof of Proposition 1. We start with another identity. If the natural number n^* is a multiplicative inverse of $n \bmod b$, i.e., $nn^* \equiv 1 \bmod b$, then

$$S(n^*, b) = S(n, b).$$

This equation is equivalent to formula (4a) in [3] and easy to verify (use (6)). It shows that $S(2, b) = S((b+1)/2, b)$ for odd numbers b. In this case the reciprocity law (8) yields $S(2, b) = (b^2-1)/12$.

Next we show

$$S(n, b) > (b^2-1)/12 \qquad \text{if} \quad 2 < n < (b+1)/2 \tag{18}$$

and

$$S(n, b) < (b-1)(b-3)/4 \qquad \text{if} \quad 1 \leqslant n < (b-1)/2. \tag{19}$$

Since $(b-1)(b-3)/4 = (b-1)(b-2)/3 - (b^2-1)/12$, the complement formula, applied to (19), gives $S(n, b) > (b^2-1)/12$ for $(b+1)/2 < n \leqslant b-1$. Together with (18) this proves the proposition.

In order to prove (18) we may assume $b \geqslant 4$. We define the polynomials

$$P_b(X) = (b-1)(X-1)(b+X-1)/6,$$

$$Q_b(X) = P_b(X) - b(X-1)(X-2)/3 - (b^2-1)\,X/12$$

in $\mathbb{Q}[X]$. The quadratic polynomial Q_b has $-(b+1)/6$ as its leading coefficient and the (distinct) rational zeros 2 and $(b+1)/2$ (>2), as a short calculation shows. Therefore $Q_b(x)$ takes positive values for all x with $2 < x < (b+1)/2$ (and nonpositive values outside this interval). In particular,

$$P_b(n) - b(n-1)(n-2)/3 > n(b^2-1)/12 \tag{20}$$

holds for all integers n with $2 < n < (b+1)/2$. But by the reciprocity law (8) and by (17),

$$nS(n, b) = P_b(n) - bS(b, n) \geqslant P_b(n) - b(n-1)(n-2)/3.$$

Together with (20), this implies (18). The proof of (19) is similar: Define

$$R_b(X) = P_b(X) - (b-1)(b-3)\, X/4.$$

This polynomial has -2 and $(b-1)/2$ as its zeros and takes negative values for all x with $-2 < x < (b-1)/2$. Now the reciprocity law, together with (16), gives (19). ∎

Remark. It is easy to transform all results of this section into results for the sums

$$T(b, n) = \sum_{k=1}^{n-1} k(kb)_n,$$

which are of interest for their own.

ACKNOWLEDGMENT

The author thanks the referee for his helpful comments.

REFERENCES

1. K. Girstmair, Periodische Dezimalbrüche—was nicht jeder darüber weiss, *in* "Jahrbuch Überblicke Mathematik 1995," Vieweg, Braunschweig, 1995.
2. C. Meyer, Über einige Anwendungen Dedekindscher Summen, *J. Reine Angew. Math.* **198** (1957), 143–203.
3. H. Rademacher, Zur Theorie der Dedekindscher Summen, *Math. Z.* **63** (1956), 445–463.
4. H. Rademacher, "Topics in Analytic Number Theory," Springer-Verlag, Berlin, 1973.
5. H. Rademacher and E. Grosswald, "Dedekind Sums," (Carus Mathematical Monographs, No. 16), Math. Assoc. Amer., Washington, DC, 1972.